IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
Plaintiff,	)	Civil Action No. 16-1780
v.	)	
"flux"	)	
a/k/a "ffhost,"	)	
	)	
and,	)	
	)	
"flux2"	)	
a/k/a "ffhost2"	)	
Defendants.	)	

FOURTH SIXTY DAY REPORT

The United States of America, by and through its attorneys Soo C. Song, Acting United States Attorney for the Western District of Pennsylvania and Kenneth A. Blanco, Acting Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Richard D. Green, Senior Trial Attorney, respectfully provides this Fourth Sixty Day Report in support of the Preliminary Injunction granted and issued by this Court on December 9, 2016, against Defendants "flux" and "flux2."

1. On December 9, 2016, this Honorable Court issued a Preliminary Injunction on the motion of undersigned counsel designed to prevent the fraud being perpetrated on hundreds of thousands of victims world-wide by the defendants. (Dkt. No. 17).

2. The defendants administer a hosting infrastructure known as "Avalanche" comprised of a worldwide network of servers controlled by through a highly organized central control system. The Avalanche administrators rent out access to the Avalanche network to cyber criminals for the bulletproof hosting services over which the malware attacks and money mule campaigns victimize hundreds of thousands of people throughout the world.

3. The injunctive relief Order by this Honorable Court on December 9, 2016, commanded the defendants to stop using Avalanche to defraud and wiretap American citizens and businesses. To give effect to that prohibition, this Honorable Court authorized the United States to employ a series of technical measures designed to disrupt the defendants' infrastructure and related malware systems. Specifically, this Honorable Court authorized the United States to: (1) direct certain U.S. Domain Registries to redirect proscribed a list of domain names used by Avalanche or the malware systems that traverse it to substitute servers and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); (2) direct certain U.S. Domain Registries to cause a separate list of domain names to block access to a proscribed list of domain names used by Avalanche or the malware systems that traverse it and, at the registries' discretion, to register those with the Registry of Last Resort (RoLR); (3) direct certain U.S. Domain Registries to register a proscribed list of domain names, direct them to substitute servers, and, at the registries' discretion, transfer the domain names to the Registry of Last Resort (RoLR); and (4) direct certain U.S. Domain Registries to transfer a proscribed list of domain names and redirect them to substitute servers. (Dkt. No. 17).

4. In addition to the civil relief described above, this Honorable Court also authorized the United States to utilize a Pen Register/Trap and Trace Order that collects the dialing, routing, addressing, and signaling information of communications sent by the computers infected with Avalanche or the malware systems that traverse it to the substitute servers and other computer infrastructure established pursuant to the TRO sought by the Government. This information is disseminated to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the ShadowServer Foundation, the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) to facilitate the notification of

Avalanche victims and provide instruction on how to remove these infections from their computers.

5. At the time this Honorable Court granted the equitable relief, the United States advised the Court that it would report on the progress of the sinkholing operations every sixty (60) days. The United States submits the Fourth Report in continued conformance with that obligation.

6. The sinkholing operation has been quite successful in its effectiveness. Currently, the operation continues to sinkhole approximately 70,000 new Internet Protocol (IP) addresses each day. The consistency of these numbers is attributable to the lack of new remediation by victims. These IP addresses continue to be located throughout the world. Given the profoundly disabling impact on Avalanche and the malware families that traverse, the United States will continue its sinkholing operation consistent with the scope of the equitable relief granted by this Honorable Court.

7. The United States will report again to this Honorable Court no later than October 2, 2017.

Respectfully submitted,

SOO C. SONG
Acting United States Attorney

By: /s/ Michael A. Comber
MICHAEL A. COMBER
Assistant U.S. Attorney
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

KENNETH A. BLANCO
Acting Assistant Attorney General

By: /s/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov